



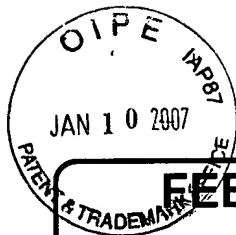
AFZM

TRANSMITTAL FORM (to be used for all correspondence after initial filing)		Application No.	09/672,368
		Filing Date	September 28, 2000
		First Named Inventor	Francis X. McKeen
		Art Unit	2132
		Examiner Name	Ho, Thomas M.
Total Number of Pages in This Submission		Attorney Docket Number	42390P9575

ENCLOSURES (check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form <input checked="" type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> PTO/SB/08 <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/Incomplete Application <input type="checkbox"/> Basic Filing Fee <input type="checkbox"/> Declaration/POA <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">-Check for \$500.00 -Return postcard</div>
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Gregory D. Caldwell, Reg. No. 39,926 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	January 8, 2007

CERTIFICATE OF MAILING/TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			
Typed or printed name	Katherine Jennings		
Signature		Date	January 8, 2007



FEE TRANSMITTAL for FY 2006

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT (\$) 500.00

Complete if Known

Application Number	09/672,368
Filing Date	September 28, 2000
First Named Inventor	Francis X. McKeen
Examiner Name	Ho, Thomas M.
Art Unit	2132
Attorney Docket No.	42390P9575

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below

☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☒ Credit any overpayments

FEE CALCULATION

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
Other fee (specify) _____					
				SUBTOTAL (2)	(\$) 500.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Gregory D. Caldwell	Registration No. (Attorney/Agent)	39,926	Telephone	(310) 207-3800
Signature		Date	01/08/07		

TABLE OF CONTENTS

I.	Real Party in Interest	1
II.	Related Appeals and Interferences	1
III.	Status of Claims	1
IV.	Status of Amendments	1
V.	Summary of Claimed Subject Matter	1
VI.	Grounds of Rejection To Be Reviewed On Appeal	3
VII.	Argument	3
A.	Overview of Cited References	4
1.	<i>Distributed Systems: Concepts and Design</i> by Coulouris <i>et al.</i> ("Coulouris")	4
2.	<i>Operating System Concepts</i> by Silberschatz <i>et al.</i> ("Silberschatz")	4
3.	U.S. Patent No. 6,098,133 to Summers <i>et al.</i> ("Summers")	4
4.	U.S. Patent No. 5,615,263 to Takahashi (" <i>Takahashi</i> ")	4
B.	Claim 1: Isolated Execution Method	5
C.	Claim 9: Apparatus Generating Isolated Access Bus Cycles	8
D.	Claim 12: Platform Including Isolated Execution Circuit	9
VIII.	Claims Appendix	11
IX.	Evidence Appendix	15
X.	Related Proceedings Appendix	16



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:) Examiner: Ho, Thomas M.
Francis X. McKeen, Lawrence O.) Art Group: 2132
Smith, Crawford Chaffin Benjamin,)
Michael P. Cornaby, and)
Bryant Bigbee)
Application No. 09/672,368)
Filed: September 28, 2000)
For: MECHANISM TO HANDLE EVENTS IN)
A MACHINE WITH ISOLATED)
EXECUTION)

Assistant Commissioner for Patents
Board of Patent Appeals and Interferences
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.37, Applicants submit the following Appeal Brief for consideration by the Board of Patent Appeals and Interferences ("Board"). Applicants also submit herewith a check in the amount of \$500.00 to cover the cost of filing this opening brief, as set forth in 37 C.F.R. § 41.20(b)(2). Please charge any additional amounts due or credit any overpayment to Deposit Account No. 02-2666.

I. REAL PARTY IN INTEREST

Francis X. McKeen, Lawrence O. Smith, Crawford Chaffin Benjamin, Michael P. Cornaby and Bryant Bigbee, the parties named in the caption, transferred their rights in that which is disclosed in the subject application through an assignment to Intel Corporation recorded as reel/frame number 018706/0579. Intel Corporation is the owner at the time this brief is filed, and therefore is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-15 are pending in this application. All claims stand rejected. Claims 1-15 are presented for appeal based on arguments in support of independent claims 1, 9 and 12.

IV. STATUS OF AMENDMENTS

All amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention concerns platforms and methods to handle asynchronous events in a secure manner (p. 2, l. 4; p. 3, ll. 6-7). Embodiments can help prevent data "leaks," where secure information inadvertently becomes exposed to untrusted software (p. 3, ll. 6-14). This is accomplished by establishing a protected, isolated region in system memory that can only be accessed through special bus cycles (p. 5, l. 27 through p. 6, l. 3).

Independent claim 1 recites a method comprising several operations: maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode (p. 12, ll. 1-9; Fig. 2, elements 208 and 218); restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode (p. 7, ll. 3-7; p. 9, ll. 18-21); dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode (p. 12, ll. 26-30); identifying if an event is one of a class of events to be handled in the isolated execution mode (p. 13, ll. 16-20; Fig. 3, element 304); asserting a selection signal to select the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; (p. 13, ll. 25-29; Fig. 3, element 312) and handling the event using a table map selected by the selection signal (p. 13, ll. 27-29; Fig. 3, element 314).

Independent claim 9 recites an apparatus comprising several parts, including: a first storage location storing control data for a first page table map (p. 12, ll. 1-14; Fig. 2, elements 204, 206 and 208); a second storage location storing control data for a second page table map (Fig. 2, elements 214, 216 and 218); a selection unit to select which page table map is applied responsive to receipt of an event (p. 12, ll. 14-22; Fig. 2, elements 220, 222 and 224); and an isolated execution circuit to generate isolated access bus cycles (p. 8, ll. 9-18; Fig. 1C, element 115), wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode (p. 8, ll. 21-28).

Independent claim 12 recites a platform comprising several subsystems, including: a processor executing in one of normal execution mode and isolated execution mode (p. 8, ll. 9-11; Fig. 1C, element 110); a first set of control registers to define a current memory map of the platform (p. 12, ll. 10-13; Fig. 2, element 200); a mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternate memory map (p. 12, ll. 14-18; Fig. 2, elements 220, 222, 224 and 230); and an isolated

execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode (p. 8, ll. 9-19; Fig. 1C, element 115).

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claim 1 stands rejected under 35 U.S.C. § 103(a) as unpatentable over *Distributed Systems: Concepts and Design* by Coulouris, Dollimore and Kindberg (“Coulouris”), in view of *Operating System Concepts* by Silberschatz and Galvin (“Silberschatz”) and U.S. Patent No. 6,098,133 issued to Summers *et al.* (“Summers”).

Claim 9 stands rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,615,263 issued to Takahashi (“*Takahashi*”) in view of *Summers* (*supra*).

Claim 12 stands rejected under 35 U.S.C. § 103(a) as unpatentable over *Takahashi* (*supra*) in view of *Summers* (*supra*).

VII. ARGUMENT

In the Final Office Action mailed September 6, 2006 (“FOA”), the Examiner provides helpful analogies and supports his rejections with extended analyses and citations to the references of record, but his excessive use of paraphrasing and imprecise identification of claim elements with allegedly equivalent objects and principles in the references fail to satisfy the Patent Office’s burden to show that the references, taken together, would teach or suggest all of the claimed elements, arranged as recited in the claims. Careful identification and precise reasoning are especially important when, as here, the principal prior-art documents are general-purpose reference works that must be stitched together with speculative use cases and assumptions about underlying operational details.

A. Overview of Cited References

1. *Distributed Systems: Concepts and Design* by Coulouris *et al.* (“Coulouris”)

This college-level textbook describes software techniques for implementing threads, processes, virtual memory and related features in a distributed operating system. However, hardware considerations are only discussed generally and in comparative terms, so a liberal helping of speculation is required to find in the reference many of the specific technical elements recited in the claims.

2. *Operating System Concepts* by Silberschatz *et al.* (“Silberschatz”)

This is a second college-level textbook that describes software techniques for implementing features of modern operating systems using contemporary processor functionality. Like *Coulouris*, however, specific hardware considerations are not examined in *Silberschatz*, and the Examiner attributes far more detailed teachings to the reference than are actually present in the cited text.

3. U.S. Patent No. 6,098,133 to Summers *et al.* (“Summers”)

Summers describes a hardware device that can be interposed between a computer interface card and a computer bus. The device permits the interface card to be disconnected from the bus when sensitive data is being carried by the bus, so that the card cannot observe or alter the data. This has the effect of interrupting communications between the card and memory, but not in a way that satisfies the claim elements for which the reference is introduced, nor even in a way that is compatible with operations according to the references with which *Summers* is joined.

4. U.S. Patent No. 5,615,263 to Takahashi (“Takahashi”)

Takahashi describes a dual-mode processor with a secure mode and a general mode. In secure mode, the processor is only permitted to execute

instructions from an internal read-only memory ("ROM"). In general mode, instructions from a random-access memory ("RAM") may be executed. However, the processor has no virtual memory system or memory management unit, and consequently no memory map or memory map control registers. Furthermore, neither *Takahashi* nor *Summers* have a structure that generates bus cycles, let alone a structure to generate isolated access bus cycles.

B. Claim 1: Isolated Execution Method

Claim 1 recites a method comprising maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode; restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode; dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode; identifying if an event is one of a class of events to be handled in the isolated execution mode; asserting a selection signal to select the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; and handling the event using a table map selected by the selection signal.

The Examiner's analysis is somewhat difficult to follow, since it uses terms drawn from the claims, the references, and apparently from the Examiner's own knowledge, without much distinction; but as best Applicants can determine, the Examiner's position is this:

A process executing in a virtual memory system has a page table. Some page tables may be exclusive to one process, while other page tables may contain entries shared between two or more processes. An operating system ("OS") may perform a context switch from one process to another in response to a software or hardware interrupt. (Applicants agree that these general principles are correct, and are taught or suggested by *Coulouris* and *Silberschatz*, or could be found in other prior art references.)

Applying these principles to the claim elements, the Examiner seems to say that a processor executing a process with an unshared page table is the claimed isolated execution mode, and the processor executing a process with a shared page table is the claimed normal execution mode. An interrupt that causes the OS to perform a context switch from one process to another is the claimed event, and the OS somehow selects the appropriate page table for the switched-to process.

The portions of *Silberschatz* relied upon to establish the preceding operational sequence are essentially unrelated: shared and unshared page tables are discussed in connection with memory management, while interrupt-driven context switching is mentioned briefly, four chapters earlier, in connection with processes. The claimed selection signal is paraphrased out of the analysis and glossed over completely.

Now, leaving aside the question whether the execution of a process with its own page table is sufficiently different from the execution of a process with shared entries in its page table to be reasonably described as a different “execution mode,” there is still this final claim element to be considered: “restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode.” The textbooks, *Coulouris* and *Silberschatz*, do not discuss virtual memory hardware and memory access operations at the relevant level of detail, but it is commonly known that the memory protection provided by a memory management unit (“MMU”) is usually based on mapping a virtual address to a physical address using information in page tables. The physical address is then used to retrieve or store data in the memory. Of key importance here is the fact that *no different bus cycles are used whether the page table entries are shared or not*. Thus, even if *Coulouris* and *Silberschatz* did teach or suggest the various claim limitations as the Examiner alleges, there is no “hook” (explicit or implicit) to tie in an analysis of bus cycles.

Turning to the claimed isolated execution mode bus cycles, the Examiner concedes that *Coulouris* and *Silberschatz* lack consideration of the matter, but relies on *Summers* for the missing material. However, as mentioned above, there is no hook to connect *Summers*'s teachings with *Coulouris* and *Silberschatz*, so the references cannot properly be combined. Furthermore, *Summers* does not teach or suggest what the Examiner asserts it does – *Summers*'s "isolation" works differently and incompatibly to the claimed invention.

Summers describes an apparatus for isolating an untrusted peripheral from the bus of a computer when data that the peripheral should not see or affect is passing over the bus. Figure 7 shows clearly where this apparatus resides: the "secure bus arbiter" 71 is placed between the non-secure card 72 and the system backplane 75. A signal from a trusted kernel and operating system controls bus transceiver switches to isolate peripherals of one security class from the bus when data of another security class is passing over the bus (*Summers* col. 5, ll. 14-34). Even assuming that these signals caused or were associated with bus cycles performed in a particular execution mode (they do not, and are not), the apparatus isolates an untrusted *peripheral*. It does not restrict access to an isolated area of memory, as claim 1 requires.

The Examiner has proposed that *Summers*'s device could be installed to disconnect memory from the bus, but this application is not taught or suggested by *Summers*, and does not make sense. A system's memory is used by all the system's components, trusted and untrusted. The memory contains instructions for the processor, and stores data to be sent to (or received from) peripherals on the bus. If the memory was insufficiently secure to be permitted to remain connected to the bus during some transaction, then the processor would be unable to obtain instructions to perform the transaction. Even if the transaction was assumed to occur directly between two peripherals without the processor's involvement, no data associated with the transaction could come from or be stored by the system. And finally, even if all of these differences and nonsensical

operations are overlooked, there is no “bus cycle” connection to tie the pieces together: the Examiner has not identified any mechanism for restricting access to an isolated area of memory to *bus cycles* performed in the isolated execution mode. All of *Summers*’s bus cycles seem to be the same; the difference is whether the untrusted peripheral can observe the bus during a bus cycle.

For at least the foregoing reasons, the Board should overturn the Examiner’s rejection of claim 1.

C. Claim 9: Apparatus Generating Isolated Access Bus Cycles

Claim 9 recites an apparatus comprising a first storage location storing control data for a first page table map, a second storage location storing control data for a second page table map, a selection unit to select which page table map is applied responsive to receipt of an event, and an isolated execution circuit to generate isolated access bus cycles, wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode. The Examiner rejected this claim as obvious over the dual-mode (“general/external mode” and “secure/internal mode”) processor described in *Takahashi*, in view of the bus-transceiver apparatus of *Summers*.

Takahashi does not teach any sort of page table map or a selection unit to select which page table map is applied responsive to receipt of an event. Instead, *Takahashi*’s processor executes instructions from an internal read-only memory (“ROM”) when it is in secure mode, and executes instructions from an external random access memory (“RAM”) when in general mode. A hardware control circuit prevents the execution of RAM instructions in secure mode, but this is different from selecting one of two page maps.

Furthermore, *Takahashi* lacks any sort of isolated execution circuit to generate isolated access bus cycles if the apparatus operates in an isolated execution mode. (In *Takahashi*’s secure mode, RAM can still be accessed to obtain data, but no distinct type of bus cycle is described or implied.) Again, the

Examiner turns to *Summers* for its isolation of untrusted peripherals, but as explained above, the secondary reference does not generate or use isolated access bus cycles either.

For at least these reasons, the Board should overturn the Examiner's rejection of claim 9.

D. Claim 12: Platform Including Isolated Execution Circuit

The final independent claim presented for review, claim 12, recites a platform comprising a processor executing in one of normal execution mode and isolated execution mode, a first set of control registers to define a current memory map of the platform, a mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternate memory map, and an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode. The Examiner rejected this claim over *Takahashi* and *Summers*, allegedly finding the different elements of this claim in the same portions of the references that were cited in the rejection of claim 9. However, *Takahashi* lacks control registers to define a current memory map, or anything remotely like such registers; indeed, it lacks even the concept of a memory map. Furthermore, even assuming (solely for the sake of argument) that *Takahashi*'s RAM and ROM could reasonably be described as different memory maps, neither of the references teach or suggest an isolated execution circuit to generate isolated access bus cycles.

The Board should reverse the Examiner's rejection of claim 12, and hold that this claim is allowable.

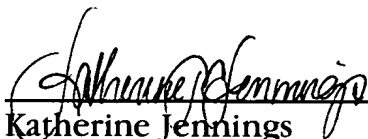
Conclusion

Based on the foregoing, Applicants request that the Board overturn the rejection of all pending claims and hold that all of the claims currently under review, and all claims that depend therefrom, are allowable.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Dated: 1/9, 2007


Gregory D. Caldwell, Reg. No. 39,926

<p>12400 Wilshire Boulevard Seventh Floor Los Angeles, California 90025 (310) 207-3800</p>	<p style="text-align: center;"><u>CERTIFICATE OF MAILING</u></p> <p>I hereby certify that the correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail, in an envelope addressed to:</p> <p style="text-align: center;">Assistant Commissioner for Patents Board of Patent Appeals and Interferences P.O. Box 1450 Alexandria, VA 22313-1450</p> <p> <u>1-8-07</u> Katherine Jennings Date</p>
---	---

VIII. CLAIMS APPENDIX

The claims involved in this appeal are presented below.

1. (Previously Presented) A method comprising:
 - maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode;
 - restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode;
 - dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode;
 - identifying if an event is one of a class of events to be handled in the isolated execution mode;
 - asserting a selection signal to select the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; and
 - handling the event using a table map selected by the selection signal.
2. (Previously Presented) The method of claim 1 further comprising:
 - identifying if the event is one of a class of events to be handled in the isolated execution mode; and
 - handling the event using the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode;
 - wherein identifying comprises indexing into a lookup table with a exception vector of the event.
3. (Original) The method of claim 1 wherein dynamically swapping comprises:
 - loading a set of control registers selected based on an exception vector of the event.

4. (Original) The method of claim 3 wherein the set of control registers comprises:
 - a global descriptor table register;
 - an interrupt descriptor table register; and
 - a page table map base address register.
5. (Original) The method of claim 1 wherein maintaining comprises:
 - mirroring a page table base address register.
6. (Original) The method of claim 1 further comprising:
 - defining a set of events that should be handled in isolated execution mode.
7. (Original) The method of claim 6 wherein the set of events to be handled in the isolated execution mode comprises:
 - machine check events and clock events.
8. (Previously Presented) The method of claim 1 wherein handling comprises:
 - determining if a current mode is the isolated execution mode;
 - loading a set of control registers with values corresponding to the first page table map if the current mode is not the isolated execution mode and the event is one of the class; and
 - dispatching an exception vector after the loading is complete.
9. (Previously Presented) An apparatus comprising:
 - a first storage location storing control data for a first page table map;
 - a second storage location storing control data for a second page table map;
 - a selection unit to select which page table map is applied responsive to receipt of an event; and
 - an isolated execution circuit to generate isolated access bus cycles,

wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode.

10. (Original) The apparatus of claim 9 wherein the selection unit comprises:
a multiplexer that selects between the first and the second storage locations based on an exception vector of the event.

11. (Original) The apparatus of claim 9 wherein the first storage location contains a base address for the first page table map and the second storage location contains a base address for the second page table map.

12. (Previously Presented) A platform comprising:
a processor executing in one of normal execution mode and isolated execution mode;
a first set of control registers to define a current memory map of the platform;
a mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternate memory map; and
an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode.

13. (Original) The platform of claim 12 wherein the mapping unit comprises:
a second set of registers having a first subset corresponding to control register values for a normal execution mode memory map and a second subset corresponding to control register values for an isolated execution mode memory map; and
a selection unit to select between the first subset and the second subset.

14. (Original) The platform of claim 13 wherein the selection unit comprises:

a plurality of multiplexers having selection driven by an exception vector of an incoming event.

15. (Original) The platform of claim 12 wherein the first set of control registers comprises:

- a global descriptor table register;
- an interrupt description table register; and
- a page table map base address register.

16. – 30. (Canceled)

IX. EVIDENCE APPENDIX

No evidence is attached.

X. RELATED PROCEEDINGS APPENDIX

No related appeals, interferences or judicial proceedings are known.